PROCEDURE 1310.02
Issued: January 1, 1994

SUBJECT: Information processing security.

APPLICATION: Executive Branch Departments and Sub-units.

PURPOSE: To provide the procedures to secure and protect State information processing facilities, data and media, software, hardware and personnel.

CONTACT AGENCY: Department of Information Technology (DIT)
Office of Research and Policy

TELEPHONE: 517/373-7326

FAX: 517/335-2355

SUMMARY: The procedures are designed to cover all pertinent responsibilities that relate to information processing security. Because of this, certain guidelines are not the direct responsibility of the information processing manager and may require coordination with other external agencies.

APPLICABLE FORMS: As required.

PROCEDURES:

Instruction A: Mainframe and General Information Processing

Agency insures that:

- Physical site:
  - In a multi-storied building, the computer room must be located above the first floor (applies to newly constructed computer rooms only).
  - A computer room will not be located adjacent to exterior walls or near building entrances (applies to newly constructed computer rooms only).
  - Fire resistant walls, ceiling, doors, and flooring must surround the computer room. Computer room walls must not contain windows if they are part of the building exterior (applies to newly constructed computer rooms only).
  - In multi-storied buildings, the floor above the computer room must be made water tight (applies to newly constructed computer rooms only).
  - The computer room must be equipped with smoke and heat detectors as determined by the appropriate fire regulations.

- Remote switches, other than the actual machine on/off switches to shut off all installation power, must be installed near the entrance or exit of the computer room.

- Approved portable extinguisher, per Fire Marshal specifications, must be available and clearly marked.

- Emergency lighting is mandatory.

- All equipment that requires grounding must be grounded.

- Walls must extend from structural floor to structural ceiling in computer room where room construction features permit.

- Drains must be installed under raised floors and water detectors must be used (applies to newly constructed computer rooms only).

- Entrance and exit doors must remain locked and equipped with alarms.

- Raised floor panel lifters must be available.

- Fire and smoke detectors, fire extinguisher, alarms, emergency exits, and alternative power supplies must be tested and maintained.

- Evacuation route floor plans must be posted in conspicuous locations.

- Circuit breaker panels must be located in a secure area and their locations marked.

- Manually operated alarm locations must be easily accessible and conveniently located.

- Define and document how and who Building Management must notify in case of any scheduled or emergency interruption in service for the following:

  -- Electrical power
  -- Water service
  -- Environment
  -- Drainage service

- Each data center must develop and issue procedures for emergency interruptions in service and make periodic tests to ensure that the procedures are effective.

- Written procedures to provide a secure computer room must include:

  -- Who is authorized in the computer room during prime and non-prime shifts and how are they to be recognized and admitted.

  -- Restrictions on eating, drinking, and smoking in the computer room.

- All guided tours of the information processing facility must be pre-scheduled. No unguided tours will be conducted.

- Environmental conditions must be defined and documented for the computer room as must the person who is responsible for monitoring them.

- The primary file library area must be designed as a restricted area and must not have windows or public access.

- An off-site back-up file library or vault must be utilized which is a minimum of 5 miles from the main processing site.

- If a vault is used for security, the vaults must remain closed and locked except when materials are being removed or placed in vaults.

- Each department must designate a primary and secondary location for all production systems documentation to include back-up copies of operation guides.

- Written procedures must exist for original issues as well as lost stolen, or forgotten keys, cards, and badges used to access the computer room.

• Software controls:

- Terminals must not display passwords when keyed.

- System software must protect passwords or other security information.

- Security violations must be logged.

- Security violation log must be reviewed and problems resolved.

- Terminals must be automatically logged off after repeated attempts to gain access or if left unattended for a specific period of time.

- Procedures must be established and implemented for controlling dial-in access to a computer system.

- Production program and data files must be protected against unauthorized access.

- Telecommunications software must generate terminal usage reports to data center management.

- Passwords must be assigned in a secure manner, periodically changed, and promptly deleted for terminated employees.

- Security requirements and procedures must be documented and approved by management for each application system.

- Procedures must be established and implemented for monitoring computer console (ODT) activities for the purpose of identifying security and procedural violations.

- Procedures must be established and implemented for scheduling all jobs through the computer system. Special requests must be authorized before the job is run.

- Execution reports or other reports must be reviewed to ensure jobs are run correctly.

- A written request must be given to the appropriate organizational unit prior to modifying production programs.

- Data center management must require all system software changes to be documented and approved.

- System utilities, which override or bypass controls, must not be used unless approved by data center management.

• Data and media:

- All master and transaction files (necessary for update of master files) must have at least one back-up file. If feasible, 2 back-up files should be available. (A back-up file may be a duplicate file, first or second generation file.)

- Written procedures must be established for the file librarian and must contain the following:

  -- Physical security procedures.

  -- Who is authorized and channels through which files can be released.

  -- Log in and out procedures for all files going outside the installation.

  -- Back-up file procedures.

  -- Emergency interruption of service procedures.

  -- Person who knows the safe combination.

  -- Retention cycle procedures.

- Each production file must have a unique, approved file identification (ID) number on the gummed label and on the header label. This unique ID number must begin with a 1-digit State department code, thus eliminating any duplicate ID numbers.

- Each tape and removable disk must have an assigned serial number.

- Tape containers, seals, or pack containers must be used during all non-machine processing periods.

- File protect rings must be removed from all tape files to be saved.

- Confidential reports must be labeled as being confidential or containing proprietary information and must remain in a secure area until picked up by an authorized user.

• Personnel:

- An individual must be designated as the security officer for each site or installation.

- A security check must be made on all new personnel hired to work in a data center prior to employment.

- Computer operations functions must be organizationally separated from computer operations and applications programming functions.

• Miscellaneous:

- Authorized signatures must be required when releasing confidential information.

- All contracts involving outside contractors must contain a security clause if the contractor is to have access to confidential data and/or to the data center itself.

- Erroneously created confidential information must be shredded or otherwise destroyed.

- Confidential documents, forms, and negotiable documents must be stored, controlled, and periodically inventoried.

Instruction B: End-user Computing (EUC) Security

All departments and agencies shall have the responsibility for managing the security of resources associated with End User Computing (EUC).

• General:

Internal policies and procedures must be developed to address the following EUC security issues:

- An individual must be designated as EUC Security Officer with responsibility for:

-- Implementing and enforcing security policies and procedures.

-- Regularly reviewing EUC security effectiveness.

-- Reviewing and recommending to data center management any changes to EUC security policy and procedure.

- Ensuring the compatibility and consistency with other data center and departmental policies and procedures.

- Performing regular (and random) site inspections and user reviews to verify:

  -- Physical inventories.

  -- Environmental conditions.

  -- General compliance with EUC policies and procedures.

  -- Training and communications (to ensure awareness of EUC policies as well as operational information).

  -- Service request process (to track and prioritize needs and problems associated with EUC).

• Physical Security:

  Internal policies and procedures must be developed to address the following physical security issues:

  - Central identification and inventory of all hardware, including regular and random physical inventory checks.

  - Location and movement of any and all EUC equipment.

  - Connection or disconnection of any and all EUC equipment.

  - Site and environment requirements or restrictions.

  - Maintenance and service.

  - Identifications of all valid users and conditions of access.

  - Media protection procedures with specific concern for hard disk storage units.

• Software Security:

  Internal policies and procedures must be developed to address the following software security issues:

  - Identification and periodic review of any and all license agreements associated with all software.

  - Informing and training users of their responsibility regarding license restrictions and software usage (e.g., copy restrictions).

- Central identification and inventory of all software authorized to be used and supported on EUC equipment.

- Internal software development policy (procedures to describe any and all restrictions to be placed on internally developed application software including programming standards, languages and support).

- Support and assistance procedures.

- Data Security:

  Internal policies and procedures must be developed to address the following data security issues:

  - Identification of data owners.

  - Data maintenance and release (data owners define the procedures for use by others).

  - Documentation, backup, and recovery procedures.

  - Local data vs. inter divisional or departmental data.

  - Confidential or sensitive data.

- Networks:

  Internal policies and procedures must be developed to address the following:

  - Standards and conditions for any and all local area network hardware and software.

  - Standards and conditions for any and all in-house mainframe connections.

  - Access to external networks and mainframes.

  - Communications software.

  - Installation and access to modems and data communications lines.

* * *